AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

11 Feb 2013
Product #: CRIM-0006-13

AFOSI SPECIAL PRODUCT

(U) Cybersex Extortion Scams

"Sextortion"

(U) Cybersex Extortion Scams

(U) INFORMATION CUTOFF DATE: 5 February 2013

(U) PREDICATION

(U) This Special Product was produced in response to reports of Department of Defense (DoD) personnel becoming victims of internet-based extortion scams known as sextortion. Its purpose is to inform United States Air Force (USAF) personnel of this new online scam and offer mitigating steps that can reduce the chances of becoming a victim.

(U) INTRODUCTION

(U) Cyber criminals are continually developing new online scams to take advantage of the unsuspecting public. One of the most recent is cyber sextortion. Cyber sextortion generally refers to an act of using sexual images (obtained either through enticement or malicious code) in order to extort money from unsuspecting victims.

(U) Reporting across Military Services indicates that DoD personnel have been subjected mainly to webcam sextortion scams. DoD personnel were enticed to engage in online sexual activities which were secretly recorded; money was then extorted from the victims in order to prevent the release of compromising video material. Reported instances of sextortion involving DoD personnel suggests that many of the perpetrators originate from the Philippines. It is currently unclear whether perpetrators are specifically targeting US military members or whether DoD and USAF personnel are merely victims of a scam directed at the general public. Nonetheless, USAF personnel should be vigilant about protecting their personal information online and refrain from engaging in sexual activities through the internet that may potentially make them vulnerable to extortion.

(U) MECHANICS OF SEXTORTION SCAMS

(U) Cyber criminals involved in sextortion scams generally pose as attractive females seeking friendly conversation. They approach potential victims in chat rooms, popular dating websites, and social networking sites by initiating written/text communication in an attempt to befriend them. To convince an unsuspecting individual the person they are about to befriend is real, the perpetrator posts fictitious information about themselves (usually age, location, and multiple photos of the same person) to help establish legitimacy.[1]

(U) Once the victim has accepted the perpetrator's friendship invitation, the "online relationship" commences and perpetrators quickly change the nature of the conversation from friendly to sexual. At this point victims are invited to participate in live video communication and are lured into cybersex activities.

(U) In many cases perpetrators enact sexually explicit poses or engage in masturbation to entice the victim to reciprocate. Perpetrators then inform unsuspecting victims that their online sexual activities have been recorded. The perpetrator subsequently threatens to upload the contents on various websites (YouTube,

Facebook, heterosexual and homosexual porn sites, etc.) or distribute it to the victims' family, friends, or coworkers unless financial payment is made. In some instances victims were forced to purchase a subscription to pornographic websites.[2] Those websites provide financial incentives similar to "referral fees" for perpetrators who coerce victims to sign up for the service.

(U) Monetary demands placed on the victims have averaged around several hundred dollars (US$) per person. In one case, however, law enforcement authorities in Singapore broke up a sextortion ring responsible for extorting upward of US$90,000 from a single victim over a 9-month time period. The authorities suspected the same group deprived another individual of nearly US$100,000 by threating to make victim's cybersex activities public.[3]

(U) SEXTORTION CASES INVOLVING DOD MEMBERS

(U) Currently it is not known how many DoD personnel have been victimized by this type of online sextortion scam. In November 2012, Facebook's security team—the world's largest social networking site—identified a major sextortion ring operating out of Naga City, Philippines. The ring, involving 21 employees of the Philippine-based company MoneyMaker Portal Web Solutions, reportedly targeted hundreds of US Army and Navy members for a period over one year.[4] It is unknown how many DoD members were actually victimized by this ring. Less dramatic examples of cyber criminals targeting DoD members through these types of scams have been observed by all Military Criminal Investigative Organizations.

(U//FOUO) A recent Naval Criminal Investigative Service (NCIS) report focusing on this type of online scam identified four cases (two on Guam, one in Japan, and one in Bahrain) involving Navy members between August 2012 and November 2012. In all instances, Department of the Navy personnel were lured into online sexual activity that was secretly recorded, and were subsequently threatened with exposure if payment was not made.[5] The United States Army Criminal Investigation Command (USACIDC) also reported a total of three cases from South Korea, Germany, and Texas, of Army members who were recently victimized. In all cases, victims engaged in consensual cybersex activities that were secretly recorded and subsequently used to extort money from them.[6] AFOSI has also received multiple reports indicating that USAF personnel have been subjected to sextortion scams. Multiple incidents of sextortion involving USAF members were reported in Japan, South Korea and Alaska, one in Portugal, and one on Guam.

(U) PROFILE OF THE PERPETRATORS

(U) Although it is currently difficult to ascertain the profile and origins of the perpetrators involved in these scams, many of appear to be connected to the Philippines. Some perpetrators have also been arrested in Singapore.[7]

(U) WHY DoD MEMBERS

(U) The Department of Justice and the Department of State identified online dating and romance scams as a significant concern to all US citizens.[8] Currently it is not known if these types of scams specifically target military members; however, DoD members could pose a target for online criminals because they may be perceived as more vulnerable to blackmail and extortion. The expectation to maintain a professional

appearance, coupled with the strict requirements associated with maintaining a security clearance, could make DoD members valuable targets for online sextortion scammers.

(U) MITIGATION

(U) While cyber criminals will continue to plague social networking websites and look for unsuspecting victims, there are measures that can be taken to avoid becoming a victim to these types of scams. All DoD members should be vigilant in protecting their personal information and limit what information they divulge on social networking sites. Listed below are some steps DoD members can take to reduce their chances of becoming a victim of sextortion scams:

- Ensure your computer is up-to-date. The operating system, antivirus and security software, and web browser plugins should be regularly checked for updates.
- Protect your personal information, especially financial and personal data. (Such as credit card details, bank account numbers, home and work addresses, etc.)
- Never send money or financial details to individuals without confirming their identity.
- Know with whom you are communicating. (Confirm details that are not publically available or posted on social networking sites.)
- Do not respond to unsolicited e-mails or chat requests; the best approach is to delete the e-mail or ignore chat requests. (When you send a message, even if it is a negative message, you are acknowledging that you read the message and that your e-mail address is valid. This can make you vulnerable to malicious software being directed at your e-mail address, or similar electronic accounts.)
- A request to exchange provocative pictures or videos should be an immediate indicator of a potential scam (Report the message to the website administrator. The wording on every website will vary, but it is often similar to "Report this message" or "Flag this as a phishing attack".)
- Be aware of activities that are out of place for the people you know. (If your friend's activities seem suspicious, you may want to contact them through alternative means such as a cellphone or government e-mail address.)

(U) Additionally, AFOSI has previously produced products in regard to protecting personal information online. Please reference "Online Impersonations of DoD Personnel," and "Guidance on Reducing USAF Members' Internet Footprints and Protecting Online Information."[9,10]

(U) If individuals believe they may have fallen victim to this type of scam, they should immediately report it to the local AFOSI detachment and chain-of-command (or security officer as appropriate). Additionally, victims of these scams can file a complaint with the Internet Crime Complaint Center, a joint task force established between the FBI and the National White Collar Crime Center, at www.IC3.gov.

ADMINISTRATIVE

(U) Author: Brenda Jones, AFOSI ICON/ICR, (571) 305-8543, Dejan Dedic, AFOSI ICON/ICR (571) 305-8796.
(U) Coordinated with: The Naval Criminal Investigative Service and the United States Army Criminal Investigation Command.

(U) All headings without classification markings are unclassified.

(U) Please send your feedback, comments, or suggestions to AFOSI/ICON/CRIMINAL INTEGRATION DESK, Brenda Jones, AFOSI ICON/ICR, brenda.jones@ogn.af.mil and Dejan Dedic, AFOSI ICON/ICR, dejan.dedic@ogn.af.mil.

(U) REFERENCES

[1] Criminal Intelligence Report – Cyber Sex Scams, AFOSI Detachment 581, 24 Jan 13.
[2] "Sextortion – MoneyMaker Portal Web Solutions," Facebook Security Incident Response Team, Undated.
[3] "Singaporean loses $97,000 in online cybersex scam," Bistado, 3 Mar 2012.
[4] "Sextortion – MoneyMaker Portal Web Solutions," Facebook Security Incident Response Team, Undated.
[5] Criminal Intelligence Brief (MCIB) – 004-009-2013, NCIS MTAC, 9 Jan 13.
[6] Criminal Alert Notice 0022-13-CID101, CID, 4 Feb 13.
[7] "Singaporean loses $97,000 in online cybersex scam," Bistado, 3 Mar 2012.
[8] Internet Dating and Romance Scams, Department of State, http://travel.state.gov/travel/cis_pa_tw/financial_scams/financial_scams_4554.html (Retrieved 8 Jan 13).
[9] "Online Impersonations of DoD Personnel" AFOSI ICY, 30 Aug 2012, I2MS# 33213122261526
[10] "Guidance on Reducing USAF Members' Internet Footprints and Protecting Online Information," AFOSI ICY, 22 Jul 2011